UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

KEVIN MCGUIRE, MATTHEW WICKHAM, and AMITAI HELLER, on Behalf of Themselves and All Others Similarly Situated,

Plaintiffs,

v.

THE CRITERION COLLECTION, LLC d/b/a THE CRITERION CHANNEL,

Defendant.

Case No.: 1:24-cv-7354

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Kevin McGuire, Matthew Wickham, and Amitai Heller ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this class action complaint against defendant The Criterion Collection, LLC d/b/a The Criterion Channel ("Criterion" or "Defendant"). Criterion owns and manages a video streaming website at https://www.criterionchannel.com/ (the "Website"). On the Website, Defendant utilized a tracking pixel (the "Pixel") created by Meta Platforms, Inc. ("Meta" or "Facebook"), which were used to intercept and disclose the Website's subscribers' search terms, video watching information, and identifiable information without seeking or obtaining subscribers' consent. The Website's use of the Pixel resulted in violations of the Video Privacy Protection Act ("VPPA"), state and federal wiretap statutes, and invaded subscribers' privacy. Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who subscribed to the Website www.criterionchannel.com, owned and operated by Defendant.

2. The Website offers subscribers the ability to pay money, or otherwise obtain a 7-day free trial, to obtain a membership to Criterion Channel's streaming service.

3. A monthly subscription to the Criterion Channel costs $10.99 USD a month and an annual subscription costs $99.99 USD a year.[1]

4. This subscription unlocks access to a large collection of films, more than 500 shorts and 5,000 supplementary features, including trailers, introductions, behind-the-scenes documentaries, interviews, video essays, commentary tracks, and rare archival footage, covering an eclectic mix of classic and contemporary films from Hollywood and around the world, many not available anywhere else.[2]

5. In short, the Website's raison d'etre is providing access to and delivering pre-recorded video content.

6. Defendant chose to work with Vimeo, Inc. ("Vimeo") to host their Website and provide the streaming technology so that subscribers could digitally access Defendant's video content.

7. Defendant made use of Vimeo's "over the top" ("OTT") platform, which allows video content providers, like Defendant, to "send content over a high-speed internet connection .

---

[1] *FAQ*, CRITERION COLLECTION, https://www.criterion.com/faq/channel#:~:text=Along%20with%20the%20constantly%20refreshed,tracks%2C%20and%20rare%20archival%20footage (last visited Sept. 23, 2024).

[2] *FAQ*, CRITERION COLLECTION, https://www.criterion.com/faq/channel#:~:text=Along%20with%20the%20constantly%20refreshed,tracks%2C%20and%20rare%20archival%20footage (last visited Sept. 23, 2024). *Id.*

. . [so] users can access the content they want straight from the creator, without having to through an intermediary . . . ."[3]

8. The video content on the Website is owned and copyrighted by Defendant and, in many instances, created by Defendant themself.

9. In all instances, the web watching of these videos is tracked by Defendant as a result of its decision to place the Pixel (discussed herein) on each individual page containing Defendant's video content on the Website.

10. Defendant does not disclose that subscribers' personal identifying information ("PII")[4] would be captured by the Pixel, and then transmitted to Meta.

11. The Website does not inform subscribers that their PII will be exposed, available, and readily usable by any person of ordinary technical skill who receives that data.

12. At no point during or after the subscription sign up process – or anywhere on the Website for that matter – do Defendant seeks or obtain consent for the sharing of subscribers' PII, search terms, or the precise location of each webpage visited by subscribers, which Defendant surreptitiously gathered through the use of the Pixel that it chose to employ on the Website.

13. In today's data driven world, a company's data sharing policies for a service or subscription are important factors for individuals to consider in deciding whether to provide personal information to that service or commit to a subscription.

14. Congress has recognized the immediate and irreversible harm caused by associating and disclosing a person's personally identifiable information in conjunction with their video watching information.

---

[3] *Create an OTT platform,* VIMEO, https://vimeo.com/ott (last visited Sept. 23, 2024).
[4] 18 U.S.C. § 2710(a)(3) ("includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider").

15. Congress' enactment of the VPPA, and its continued endorsement of the statute, supports that recognition. The VPPA prohibits video tape service providers,[5] such as Defendant, from sharing subscribers' PII tied to the title, description, or subject matter of pre-recorded audio video material[6] without valid consent.[7]

16. Congress made clear that the harm to individuals impacted by VPPA violations occurs the moment, and each time, a subscriber's information is shared.

17. On the Website, because of Criterion's decision to employ the Pixel and because it chose to employ the Pixel on its video content on the Website, a subscriber's PII is shared *the moment* the subscriber requests video materials.[8]

18. Defendant purposefully implemented and utilized the Pixel, which tracks subscribers' activity on the Website and discloses that information to Facebook to gather valuable marketing data. The Pixel could not be placed on the Website without steps taken directly by or on behalf of Defendant (*see* Section B(2)).

19. To be clear, the Pixel cannot be placed on a website by Facebook. Only a website owner can place the Pixel on a website. Here, the Pixel was utilized on the Criterion Channel Website, and effectuates the sharing of subscribers' PII. None of this could have occurred without purposeful action on the part of Defendant.

---

[5] 18 U.S.C. § 2710(a)(4).
[6] 18 U.S.C. § 2710(b)(2)(D)(II).
[7] 18 U.S.C. § 2710.
[8] As defined by the VPPA, protected "personally identifiable information" includes information which identifies a person as having "*requested* or obtained" video materials. *See* 18 U.S.C. § 2710(a)(3). When a website user clicks a link leading to a video, the user "requests" authorization to access the material from the website's server and, if authorized, the server then sends the data to the user. *See How the Web works*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Getting_started_with_the_web/How_the_Web_works (last visited Sept. 23, 2024).

20. Defendant does not seek and have not obtained consent from subscribers to utilize the Pixel to track, share, and exchange their PII, search terms, and precise webpage information with Facebook.

21. When a party, such as Criterion, utilizes the Pixel, it is provided with details about its functionality, including the collection and disclosure of its subscribers' PII.[9]

22. In fact, it is made aware that one of the functions of the Pixel is to collect and share PII to "use that information to provide measurement services[] [and] target and deliver ads."[10]

23. Facebook also advises and directs website owners that there are notice and consent requirements associated with the use of the Pixel in that website owners are responsible to provide that notice and obtain those consents.

24. Not only did Criterion know that its Website's subscribers' PII would be shared, it was on notice of its notice and consent obligations.

25. Criterion cannot claim surprise as to the nature of the Pixel when Facebook itself warned Criterion, aside from needing "a clear and prominent notice on each web page where [its] Pixels are used[,]" that Criterion must "ensure, in a verifiable manner, that an end user provide[d] all necessary consents before [Criterion] use[d] [Facebook's Pixel] to enable the storage of and access to Meta cookies . . . [i]n jurisdictions that require informed consent."[11] Employing the Pixel on the Website resulted in subscribers' PII being shared with third parties, resulting in VPPA violations. Defendant, despite its use of the Pixel on the pages of the Website containing pre-

---

[9] *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools ("You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage . . . Meta[] may use cookies web beacons and other storage technologies to collect or receive information from your websites . . . .") (last visited Sept. 23, 2024).

[10] *Id.*

[11] *Id.*; *see infra* Section C(4).

recorded video content, failed to obtain subscribers' consent to allow the Pixel to operate in a way that shares subscribers' protected information with Facebook.

26. Subscribers of the Website have been harmed as a result of violations of the VPPA. In addition to monetary damages, Plaintiffs seek injunctive relief requiring Defendant to immediately (i) remove the Pixel from the Website, or (ii) add adequate notices and obtain the appropriate consent from subscribers.[12]

27. Federal and Pennsylvania legislatures addressed citizens' privacy expectations when communicating with parties over wired communications.

28. Congress passed the Federal Wiretap Act, which prohibits the unauthorized interception of electronic communications.

29. Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701 *et seq.* "prohibits the interception of wire, electronic, or oral communications, which means it is unlawful to acquire those communications using a device."[13]

30. Defendant purposefully implemented and utilized the Pixel to intercept and read subscribers' PII. Defendant knew that the Pixel would feed subscribers' PII to Facebook. The Website does not provide notice of or obtain consent as to such practices.

31. Subscribers of the Website have been harmed by Defendant, resulting in violations of the Federal Wiretap Act and WESCA. In addition to monetary damages, Plaintiffs seek

---

[12] Website owners like Criterion also have the option to anonymize the video's title within the URL or encrypt the video title using hashing, as described by Facebook. *See Meta for Developers: Advanced Matching*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching#security (last visited Sept. 23, 2024); *Meta Business Tools Terms*, FACEBOOK, https://www.facebook.com/legal/terms/businesstools ("When using a Meta image pixel or other Meta Business Tools, you or your service provider must hash [personally identifiable information] in a manner specified by us before transmission") (last visited Sept. 23, 2024).

[13] *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

injunctive relief requiring Defendant to immediately (i) remove the tracking tools from the Website, or (ii) add, and obtain, appropriate consent from subscribers.

32. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of subscribers of the Website for violations of the VPPA, 18 U.S.C. § 2710, violations of the Federal Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e), and violations of WESCA, 18 Pa. C.S. § 5701 *et seq*.

PARTIES

33. Plaintiff Kevin McGuire is, and has been at all relevant times, a citizen of Pennsylvania who resides in Pittsburgh, Pennsylvania. Plaintiff McGuire became a subscriber to the Criterion Channel in 2018 by providing payment. Plaintiff McGuire used the Website for its intended purposes to access and view video content available to Plaintiff McGuire through the Website. Plaintiff McGuire used a Chrome internet browser to view Defendant's video content while logged into his Facebook account on the same browser. Plaintiff McGuire did not consent, agree, authorize, or otherwise permit Defendant to disclose his PII to Facebook. Plaintiff McGuire was not provided with written notice that Defendant disclose its subscribers' PII, or any means of opting out of the disclosures of their PII. Still, Criterion knowingly disclosed Plaintiff McGuire's PII to Facebook. During the course of Plaintiff McGuire's subscription to the Website, Defendant collected and shared his PII with Facebook each and every time one of the Pixel Events occurred. Defendant has violated Plaintiff McGuire's right to privacy under the VPPA, the Federal Wiretap Act, and WESCA. If not for these violations of his privacy, Plaintiff McGuire would continue his use of the Website.

34. Plaintiff Matthew Wickham is, and has been at all relevant times, a citizen of Florida who resides in Vero Beach, Florida. Plaintiff Wickham became a subscriber to the

Criterion Channel in 2018 by providing payment. Plaintiff Wickham used the Website for its intended purposes to access and view video content available to Plaintiff Wickham through the Website. Plaintiff Wickham used a Chrome internet browser to view Defendant's video content while logged into his Facebook account on the same browser. Plaintiff Wickham did not consent, agree, authorize, or otherwise permit Defendant to disclose his PII to Facebook. Plaintiff Wickham was not provided with written notice that Defendant disclose its subscribers' PII, or any means of opting out of the disclosures of their PII. Still, Criterion knowingly disclosed Plaintiff Wickham's PII to Facebook. During the course of Plaintiff Wickham's subscription to the Website, Defendant collected and shared his PII with Facebook each and every time one of the Pixel Events occurred. Defendant have violated Plaintiff Wickham's right to privacy under the VPPA and the Federal Wiretap Act. If not for these violations of his privacy, Plaintiff Wickham would continue his use of the Website.

35. Plaintiff Amitai Heller is, and has been at all relevant times, a citizen of Oregon who resides in Portland, Oregon. Plaintiff Heller became a subscriber to the Criterion Channel in 2023 by providing payment. Plaintiff Heller used the Website for its intended purposes to access and view video content available to Plaintiff Heller through the Website. Plaintiff Heller used a Chrome internet browser to view Defendant's video content while logged into his Facebook account on the same browser. Plaintiff Heller did not consent, agree, authorize, or otherwise permit Defendant to disclose his PII to Facebook. Plaintiff Heller was not provided with written notice that Defendant disclose its subscribers' PII, or any means of opting out of the disclosures of their PII. Still, Criterion knowingly disclosed Plaintiff Heller's PII to Facebook. During the course of Plaintiff Heller's subscription to the Website, Defendant collected and shared his PII with Facebook each and every time one of the Pixel Events occurred. Defendant have violated Plaintiff

Heller's right to privacy under the VPPA and the Federal Wiretap Act. If not for these violations of his privacy, Plaintiff Heller would continue his use of the Website.

36. Defendant The Criterion Collection, LLC is a Delaware limited liability company with its principal place of business at 215 Park Avenue South, Floor 5, New York, NY 10003. The Criterion Collection , LLC is a New York-based home-video distribution company that is considered a leading boutique Blu-ray label. Criterion Collection started a venture called The Criterion Channel, a video streaming website featuring a mix of classic and contemporary films from Hollywood and around the world. Criterion focuses on licensing, restoring, and distributing "important classic and contemporary films."

JURISDICTION AND VENUE

37. The District Court for the Southern District of New York has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members; the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class Member is a citizen of a state different from at least one Defendant. This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 because it arises under the Video Privacy Protection Act, 18 U.S.C. § 2710, and the Federal Wiretap Act, 18 U.S.C. § 2511(1)(a)-(e).

38. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in New York, and Defendant derives revenue in the State of New York, including Defendant's revenue generated from its management over the Criterion Channel Website, including the revenue sharing, advertising sales, etc. that Defendant derives from the Website.

39. Venue is proper in the Southern District of New York pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and Defendant

conducts substantial business operations in this District. In connection with the Website, the video content, the hosting of media accessible to subscribers, and associated coding, all claims originate and arise out of the Defendant's business operations in this District.

COMMON FACTUAL ALLEGATIONS

A. Legislative Background

1. The Video Privacy Protection Act

40. "The Video Privacy Protection Act follows a long line of statutes passed by the congress to extend privacy protection to records that contain information about individuals." S. Rep. No. 100-599 at 2 (1988). Starting with the Fair Credit Reporting Act of 1970, Congress sought to protect the "confidentiality of personal information" and passed multiple laws that "expanded and [gave] meaning to the right of privacy." *Id.*

41. In 1977, Congress amended the Privacy Act, which mandated the creation of the Privacy Protection Study Commission ("the Commission"), which studied "'data banks, automated data processing programs, and information systems of governmental, regional, and private organizations, in order to determine the standards and procedures in force for the protection of personal information.'" *Id.* (quoting 95-38). The Commission concluded that an effective national information policy must: (i) minimize intrusiveness; (ii) maximize fairness; and (iii) create legitimate, enforceable expectations of confidentiality. *Id.* "As a general rule, the Commission recommended that organizations which maintained a confidential records system be placed under a legal duty not to disclose the record without the consent of the individual, except in certain limited circumstances. . . ." *Id.* at 2-3.

42. In 1988, Congress was again forced to act when a Washington-based newspaper published a profile of Judge Robert H. Bork "based on the titles of 146 films his family had rented

from a video store." *Id.* at 5. Senators took to the floor to denounce the act, with Senator Patrick Leahy noting that:

> In an era of interactive television cables, the growth of computer checking and check-out counters . . . all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch . . . I think it is something that we have to guard against.

Id. at 5-6.

43. Congress believed that these "information pools" created privacy interests that directly affected the ability of people to freely express their opinions, join in association with others, or enjoy the general freedoms and independence protected by the Constitution. *Id.* at 7.

44. As Senator Patrick Leahy and the late Senator Paul Simon recognized, records of this nature offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id.* at 7-8 (statements of Sens. Simon and Leahy, respectively).

45. Senator Simon lamented that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* at 6-7.

46. As a result, Senate Bill 2361 was drafted to "give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives" by prohibiting "unauthorized disclosures of personal information held by video tape providers." *Id.* at 6.

47. When contemplating the VPPA, Congress noted Supreme Court precedent recognizing a privacy right in the lists that reveal personal beliefs and an individual's choice of books and films. *Id.* at 4.

48. The VPPA regulates the disclosure of information about consumers' consumption of video content, imposing specific requirements to obtain consumers' consent to such disclosure. Under the statute, for each violation of the statute, a court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief, and attorney's fees.

49. The statutory damages were deemed "necessary to remedy the intangible harm caused by privacy intrusions." *Id.* at 8.

50. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1).

51. Consumer is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1). The plain language of the definition of consumer appears first among the subsections of the VPPA, and uses broad language to define what a consumer is.

52. The VPPA defines personally identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3). Here, Congress made special note that:

> The definition of personally identifiable information includes the term "video" to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of the bill. For example, a department store that sells video tapes would be required to extend privacy protection to only those transactions involving the purchase of video tapes and not other products. **This definition makes clear that personally identifiable information is intended to be transaction-oriented. It is information that identifies a particular person as having engaged in a specific transaction with a video tape service provider.** The bill does not restrict the disclosure of information other than personally identifiable information.

Senate Report 100-599, at 12 (1988) (emphasis added).

53. Congress wanted to ensure that any transaction between consumer and VTSP involving a request or procurement of specific video materials or video services would be protected. In short, the language is broad enough to encompass digital as well as physical transactions, so long as the transaction includes the defined and prohibited information.

54. A video tape service provider ("VTSP") is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

55. While 18 U.S.C. § 2710(a)(3) limits PII to information identifying a person as having requested "specific video materials or services" and 18 U.S.C. § 2710(a)(4) limits VTSP to a person in the business of renting, selling, or delivering prerecorded audio visual materials, affected consumers are not limited by any such link to "video *materials*" or "audio visual *materials."* Instead, consumer applies to "*goods* or services" from a VTSP generally.

56. The wide scope of consumer comports with the initial purpose of the VPPA, which was initially passed in 1988 for the purpose of protecting the privacy of individuals' video rental, purchase, and viewing data.

57. In 2012, Congress amended the VPPA, and in so doing, reiterated the Act's applicability to "so-called 'on-demand' cable services and Internet streaming services [that] allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones." S. Rep. 112-258, at 2.

58. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy stated that "[w]hile it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the

'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[14]

59. This application of the VPPA to modern video sources, such as websites, has been confirmed by various courts across the country.[15]

60. Defendant here is a video service provider as it provided pre-recorded audio-visual materials to Plaintiffs and Class Members on their Website.

61. The relationship between Plaintiffs and Defendant is precisely the type of relationship contemplated by the VPPA.

62. In this case, Plaintiffs' PII was knowingly and systematically disclosed to Facebook, without obtaining their consent.

2. The Federal Wiretap Act

63. The Federal Wiretap Act (the "Wiretap Act") was enacted in 1934 "as a response to Fourth Amendment concerns surrounding the unbridled practice of wiretapping to monitor telephonic communications."[16]

64. The Wiretap Act primarily concerned the government's use of wiretaps but Congress grew concerned that technological advancements like "large-scale mail operations,

---

[14] See *Committee on the Judiciary, Subcommittee on Privacy, Technology and the Law, The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century*, SENATE JUDICIARY COMMITTEE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW, *available at* https://www.judiciary.senate.gov/download/hearing-transcript_-the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21st-century (last visited Sept. 23, 2024).

[15] *See, e.g., Sellers v. Bleacher Report, Inc.,* 2023 U.S. Dist. LEXIS 131579, at *15-18 (N.D. Cal. July 29, 2023) (VPPA sufficiently applied to sports news website); *Jackson v. Fandom, Inc.,* 2023 U.S. Dist. LEXIS 125531, at *6 (N.D. Cal. July 20, 2023) (VPPA applies to gaming and entertainment website); *Louth v. NFL*, 2022 U.S. Dist. LEXIS 163706, at *11-12 (D.R.I. Sep. 12, 2022) (holding VPPA applied to NFL's videos accessible through mobile app).

[16] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022).

computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing" were rendering the Wiretap Act out of date.[17] Thus, in 1986, Congress amended the Wiretap Act through the Electronic Communications Privacy Act ("ECPA") to provide a private right of action for private intrusions as though they were government intrusions.[18]

65. The ECPA primarily focused on two types of computer services that were prominent in the 1980s: (i) electronic communications like email between users; and (ii) remote computing services like cloud storage or third party processing of data and files.[19]

66. Title I of the ECPA amended the Wiretap Act such that a violation occurs when a person or entity: (i) provides an electronic communication service to the public; and (ii) intentionally divulges the contents of any communication; (iii) while the communication is being transmitted on that service; (iv) to any person or entity other than the intended recipient of such communication.

67. While the ECPA allows a single party to consent to the interception of an electronic communication, single party consent is only acceptable where the communication is not "intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. §2511(2)(d).

[17] Senate Rep. No. 99-541, at 2 (1986).
[18] Hayden Driscoll, *Wiretapping the Internet: Analyzing the Application of the Federal Wiretap Act's Party Exception Online*, 29 WASH. & LEE J. C.R. & SOC. JUST. 187, 192 (2022).
[19] *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1103 (9th Cir. 2014).

68. While communicating with Criterion on the Website through their viewing choices, subscribers had the contents[20] of their communications with Criterion intercepted by Meta via the Pixel.

69. Criterion purposefully included the Pixel on the Website to intercept Plaintiffs' communications and redirect them to Meta to improve the effectiveness of its and Meta's advertising and marketing.

70. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Criterion to Meta.

3. The Pennsylvania Wiretapping and Electronic Surveillance Control Act

71. Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701 *et seq.* has its roots in the common law right to privacy, which protects citizens' "protectable interest in their private information and . . . the sanctity of their communications."[21]

72. WESCA operates in conjunction with and as a supplement to the Federal Wiretap Act, which allows states to "grant greater, but not lesser, protection than that available under federal law."[22] WESCA does so.

73. WESCA prohibits: (1) the intentional interception of wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom to another person; and (3) the intentional use of

[20] The contents of Plaintiffs' and users' communications include: 1) search terms submitted to the site; 2) the location and contents of webpages visited by users; and, 3) the PII discussed in Section C(1).
[21] *Petris v. Sportsman's Warehouse, Inc.*, No. 2:23-CV-1867, 2024 WL 2817530 (W.D. Pa. June 3, 2024).
[22] *Popa v. Harriet Carter Gifts, Inc.*, 52 F. 4th 121, 124 (3d Cir. 2022).

the contents of any wire, electronic or oral communication, or evidence derived therefrom. 18 Pa. C.S. § 5703(a).

74. "Intercept" is defined as: "Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 19 Pa. C.S. § 5702.

75. WESCA defines electronic communication as: "Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature . . . ." Id.

76. Under WESCA, a court may award actual damages (but not less than liquidated damages computed at the rate of $100 a day for each violation of the statute, or $1,000, whichever is higher), punitive damages, equitable relief, and attorney's fees.

77. In this case, Plaintiffs' data—their PII and video watching information—constitutes electronic communications with Criterion.

78. Plaintiffs' electronic communications with Criterion were intentionally intercepted by Criterion through the tracking methods (namely, the Pixel) that Criterion employed on the Website.

79. Plaintiffs' electronic communications were subsequently disclosed to Meta.

80. Criterion used the contents of Plaintiffs' electronic communications with Criterion, intercepted and processed by Meta, to target Plaintiffs with advertising.

81. Plaintiffs did not know of or consent to the exposure of their legally protected communications with Criterion.

82. Criterion acted with the intent to intercept, disclose, and use Plaintiffs' protected, private information for their economic benefit through the monetization of the information via targeted advertising and other means.

B. Criterion Controls The Website

1. The Criterion Collection Owns and Manages The Criterion Channel

83. Criterion maintained control over the Website.

84. While Vimeo provided the underlying technology for the Website and video streaming services, Criterion maintained control over the relevant portions of the Website.

85. "Criterion.com and CriterionChannel.com . . . are both Criterion Collection ventures."[23]

86. Criterion Collection's ownership of the Criterion Channel is reflected in its Terms of Service and Privacy Policy: "The Criterion Collection recognizes that visitors to *our* streaming service, The Criterion Channel, care about the personal information that they provide us."[24]

87. Criterion Collection's management and control does not end there. The Privacy Policy also states: "Any changes or updates to a Subscribers' personal information should be done through requests sent to channelhelp@criterion.com email or by writing to 'The Criterion Collection' in New York, NY."[25]

88. Criterion Collection claims ownership of the channelhelp@criterion.com email, noting it represents Criterion Collection's customer service department.[26]

2. Defendant Manages the Relevant Portions of the Website

[23] *FAQ*, THE CRITERION COLLECTION, https://www.criterion.com/faq/channel (last visited Sept. 23, 2024).
[24] Exhibit A, Criterion Channel Privacy Policy as of Mar. 10, 2024 (emphasis added).
[25] *Id.*
[26] *FAQ*, THE CRITERION COLLECTION, https://www.criterion.com/faq/channel (last visited Sept. 23, 2024).

89. OTT website owners have control over and choose which videos to upload and make available to their subscribers.[27]

90. OTT website owners also have control over how subscriptions work, including which videos are unlocked by subscriptions and become deliverable to subscribers.[28]

91. Vimeo provides instructions to OTT website owners, like Defendant, on how to add metadata to help users discover new and relevant video content or otherwise search within the OTT website to find videos to watch.[29]

92. Vimeo recommends, for example, naming videos to improve search engine optimization.[30]

93. Vimeo establishes that when a video is added to a OTT website by its owner or operator, the video is named after the digital file uploaded by default.[31]

94. The responsibility for providing clear titles to videos falls to the OTT website owner, which in turn, is used "to form the URL where the video lives."[32]

---

[27] *See Uploading videos on Vimeo OTT*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426966892561-Uploading-videos-on-Vimeo-OTT (last visited Sept. 23, 2024).

[28] *See Creating and Editing a Subscription*, VIMEO, *https://help.vimeo.com/hc/en-us/articles/12427127095441-Creating-and-editing-a-subscription-product-on-Vimeo-OTT* (last visited Sept. 23, 2024).*See Creating and editing a subscription product on Vimeo OTT*, VIMEO, *https://help.vimeo.com/hc/en-us/articles/12427127095441-Creating-and-editing-a-subscription-product-on-Vimeo-OTT* (last visited Sept. 23, 2024).

[29] *See Add metadata to your Vimeo OTT videos for discovery*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427018284945-Add-metadata-to-your-Vimeo-OTT-videos-for-discovery (last visited Sept. 23, 2024).

[30] *See Optimize your Vimeo OTT site for search engines (SEO)*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426994162961-Optimize-your-Vimeo-OTT-site-for-search-engines-SEO (last visited Sept. 23, 2024).

[31] *Id.*

[32] *Id.*

95. OTT website owners are given an additional opportunity to "rename a video or collection . . . URL [to] something relevant . . . ."[33]

96. OTT website owners must take affirmative steps to add detailed URLs to their OTT websites.

97. Defendant undertook these steps. Criterion added detailed URLs to the Website.

98. Vimeo gives OTT website owners the ability to add metadata to their videos "so that [their] customers can easily discover related content they might enjoy. It also allows [OTT website owners] to make it easier for viewers to find [OTT website owners'] content via search or other parameters."[34]

99. The metadata added to videos by OTT website owners can include: information about the video, like content tags that "describes the specific video"; genres; cast; crew; release date; ratings; advisories, if the video contains offending content; and advanced or custom metadata created by the OTT website owners.

100. OTT website owners must take affirmative steps to add metadata to their OTT websites.

101. Criterion undertook these steps. Criterion added metadata to the Website.

102. Vimeo informs OTT website owners – those which provide content to stream on Vimeo's OTT platforms – that Vimeo merely provides support for OTT website owners "adding conversion tracking Pixels from services like Facebook, X (formerly Twitter), or Adwords . . . ."[35]

---

[33] *Id.*

[34] *Add metadata to your Vimeo OTT videos for discovery*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427018284945-Add-metadata-to-your-Vimeo-OTT-videos-for-discovery (last visited Sept. 23, 2024).

[35] *Add tracking pixels to your Vimeo OTT checkout page*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12427502043409-Add-tracking-pixels-to-your-Vimeo-OTT-checkout-page (last visited Sept. 23, 2024).

103. Vimeo explains that "[a] pixel tracks certain events (like when someone makes a purchase through your site, etc.); when the events you're tracking are triggered, the pixel sends the data over to your analytics."[36]

104. Vimeo adds that after an OTT website owner installs a tracking pixel on their OTT website, the intercepted data is viewable on the OTT website owner's account with each pixel's platform.[37]

105. Vimeo then provides instructions to OTT website owners, like Criterion, on how to add the Pixel to their OTT Websites. OTT website owners choose whether to add tracking tools, like to Pixel, to the Vimeo-associated websites.

106. To do so, OTT website owners must first create a Pixel on Facebook's platform; and add that Pixel ID to Vimeo's tracking integration.[38] Then, the OTT website owner must attach the tracking pixel to their Associated Product in their OTT website (or otherwise select "All Products").[39] Finally, the OTT website owner must save these settings.

107. Vimeo advises OTT website owners that the Pixel tracks the following events by default: PageView, InitiateCheckout, Purchase, and Complete Registration.[40]

108. Criterion undertook the steps necessary to add the Pixel to its Website. Criterion also made use of the Pixel SubscribedButtonClick event. Criterion did not accept the default events. Instead, Criterion programmed the Pixel to collect additional information when subscribers click specific buttons, such as to request videos. *See* Section C(2).

109. Criterion controlled its Privacy Policy and cookie notifications on the Website.

---

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

110. While Vimeo provides a "simple cookie consent banner" for OTT websites, Vimeo informs OTT website owners that "[c]ertain sites may be subject to further regulations depending on their purpose, content, and user base. It is up to the site owner to determine if a site requires a more robust cookie consent banner."[41]

111. For those that want more robust cookie consent banners, OTT website owners are offered a chance to integrate "with a third-party solution to ensure legal compliance."[42]

112. Similarly, "[a]s the operator of [its] streaming service, [OTT website owners, like Criterion,] must provide [their] users with a transparent notice of how [they] handle[] their personal information, commonly known as a 'privacy policy.'"[43]

113. Vimeo provides OTT website owners with a "template that already includes the most common points of collection and uses of data for OTT streaming services." Vimeo makes clear, however, that it "makes no representation about the sufficiency or legality of the templated privacy policy" and that OTT website owners "should change the default languages depending on [their] uses of data, additional collection points, and the laws to which [their] organization[s] may be subject."[44]

114. Thus, Criterion was responsible for notifying subscribers, and obtaining their consent, yet failed to do so in accordance with the VPPA and other federal and state laws.

---

[41] *Setting up your Vimeo OTT site's cookie consent banner*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426990708241-Setting-up-your-Vimeo-OTT-site-s-cookie-consent-banner (last visited Sept. 23, 2024).
[42] *Id.*
[43] *Creating a Privacy Policy for your Vimeo OTT* site, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426965771665-Creating-a-Privacy-Policy-for-your-Vimeo-OTT-site (Sept. *Creating a Privacy Policy for your Vimeo OTT site*, VIMEO, https://help.vimeo.com/hc/en-us/articles/12426965771665-Creating-a-Privacy-Policy-for-your-Vimeo-OTT-site (last visited Sept. 23, 2024).
[44] *Id.*

C. The Criterion Channel Website Utilizes the Facebook Pixel to Gather and Transmit PII and Video Watching Data

115. Facebook offers the Pixel to web developers for the purpose of monitoring user interactions on their websites, which can then be shared with Facebook. *See supra* ¶ 21.

116. The Pixel is a marketing tool that can only be added to a webpage by website developers. A website operator must sign up for a business account or link a related Facebook account with its Pixel, and then add code to the website to make use of the Pixel.[45]

117. As Facebook notes, the Pixel must be added to each individual page that a website owner wishes to be tracked.[46]

118. Here, as discussed in Section B(2), Defendant took steps to add the Pixel to the Website via the Vimeo platform.

119. The Pixel is employed by Criterion to gather, collect, and then share user information with Facebook.[47] Receiving this information enables Facebook and the web developers to build valuable personal profiles for users, enhancing marketing effectiveness and increasing the chance of converting users into paying customers.[48] The sharing of subscribers' PII benefits Criterion by improving the effectiveness of advertising targeted at Criterion's

---

[45] *Business Help Center: How to set up and install a Meta Pixel*, FACEBOOK, *available at* https://www.facebook.com/business/help/952192354843755?id=1205376682832142 (last visited Sept. 23, 2024).

[46] *Meta for Developers: Get Started*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/get-started/ ("To install the Pixel, add its base code . . . on every page where you will be tracking website visitor actions") (last visited Sept. 23, 2024).

[47] The Facebook Pixel allows websites to track visitor activity by monitoring user actions ("events") that websites want tracked and share a tracked user's data with Facebook. *See Meta for Developers: Meta Pixel*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/ (last visited Sept. 23, 2024).

[48] *See Meta Pixel*, FACEBOOK, https://www.facebook.com/business/tools/meta-pixel (last visited Sept. 23, 2024).

subscribers. Studies have shown that personalization in digital marketing through targeted and dynamic advertising can boost revenue by 15%.[49]

120. Website owners and operators can choose to use the Pixel to share both user activity (including video watching activity) and user identity with Facebook. Here, the Criterion Channel Website shares both.

121. The harvested data can improve advertising by pinpointing audience demographics by interests, gender, or location and finding the people who are most likely to take action and view content.[50]

122. The PII harvested by Criterion provides similar, if not more, data, including the titles of videos, whether through search terms, webpage URLs, parameters, or metadata, in addition to their Facebook profile data.

123. The owner or operator of a website holds the decision-making authority over the placement of the Pixel on its site, as well as whether or not any of the data within the Pixel transmission should be "hashed" (a form of encryption).

1. The Criterion Channel Website Implemented the Pixel

124. To activate and employ a Facebook Pixel, a website owner must first sign up for a Facebook account, where specific "business manager" accounts are provided the most utility for using the Pixel.[51] For instance, business manager accounts can: (i) create and utilize more

---

[49] Wilson Lau, *What is Targeted Advertising?*, ADROLL BLOG (June 30, 2024), https://www.adroll.com/blog/what-is-targeted-advertising#:~:text=Benefits%20of%20Targeted%20Advertising,-1.%20Deliver%20a%20higher (last visited Sept. 23, 2024).

[50] *See Audience ad targeting*, META, https://www.facebook.com/business/ads/ad-targeting (last visited Sept. 23, 2024).

[51] *Business Help Center: How to create a Meta Pixel in Business Manager*, FACEBOOK, https://www.facebook.com/business/help/314143995668266?id=1205376682832142 (last visited Sept. 23, 2024).

simultaneous Pixels, (ii) manage multiple Facebook Ad Accounts and Pages from a centralized interface, (iii) access and manage multiple parties (which can then be given specific levels of access, including more easily revoking access to ex-employees), (iv) build custom audiences for multiple ad campaigns, and (v) eliminate privacy concerns related to using a personal profile for business purposes.[52]

125. To add an operational Pixel to a website, the website owner or operator must take several affirmative steps, including naming the Pixel during the creation and setup of the Pixel.[53]

126. Once the Pixel is created, the website operator assigns access to the Pixel to specific people for management purposes,[54] and must connect the Pixel to a Facebook Ad account.[55]

127. To add the Pixel to its OTT website, the website operator must follow the instructions provided by Vimeo discussed, *supra*, in Section B(2).

128. After following these steps, a website operator can start capturing and sharing information using the Pixel.

129. A Pixel cannot be placed on a website by a third-party. It must be placed directly by or on behalf of the site owner.

---

[52] Jacqueline Zote, *A step-by-step guide on how to use Facebook Business Manager* (June 14, 2021), SPROUTSOCIAL, https://sproutsocial.com/insights/facebook-business-manager/ (last visited Sept. 23, 2024).

[53] *Id.; see also* Ivan Mana, *How to Set Up & Install the Facebook Pixel (In 2022)*, YOUTUBE, *available at* https://www.youtube.com/watch?v=ynTNs5FAUm8 (last visited Sept. 23, 2024).

[54] *Business Help Center: Add People to Your Meta Pixel in Your Meta Business Manager*, FACEBOOK https://www.facebook.com/business/help/279059996069252?id=2042840805783715 (last visited Sept. 23, 2024).

[55] *Business Help Center: Add an ad account to a Meta Pixel in Meta Business Manager*, FACEBOOK, https://www.facebook.com/business/help/622772416185967 (last visited Sept. 23, 2024).

130. Once the Pixel is set and activated, it can begin collecting and sharing user activity data as instructed by the website owner.

131. When a Facebook user logs onto Facebook, a "c_user" cookie – which contains a user's non-encrypted Facebook User ID number ("UID") – is automatically created and stored on the user's device for up to a year.[56]

132. This means that for subscribers to the Website who are also Facebook users, their PII is certain to be shared. Their PII is automatically bundled with their web watching history and disclosed to Facebook when visiting a page with an active Pixel, including the home page.

133. While the process to determine what information is being collected by the Pixel from a user is admittedly complicated, the recipient of the Pixel's transmissions receives the information in a clear and easy to understand manner.

134. The seemingly complex data, such as the long URLs included in the Pixel's transmission, is "parsed," or translated into an easier to read format, such that the information is legible.

135. For example, an embedded URL in a Pixel HTTP Request may look like an indecipherable code, as depicted below:

[56] *Privacy Center: Cookies & other storage technologies*, FACEBOOK https://www.facebook.com/policy/cookies/ (last visited Sept. 23, 2024).

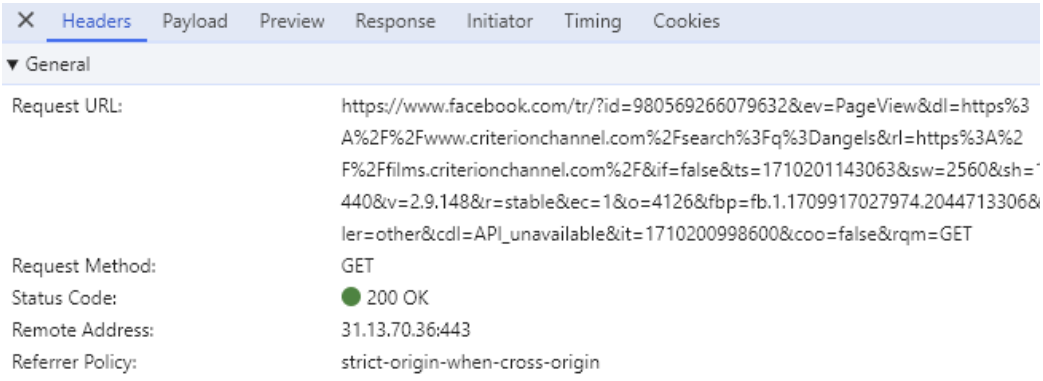

Figure 1 1 - Sample Pixel Request URL

136. However, these URLs are designed to be "parsed" into easy-to-digest pieces of information, as depicted below:

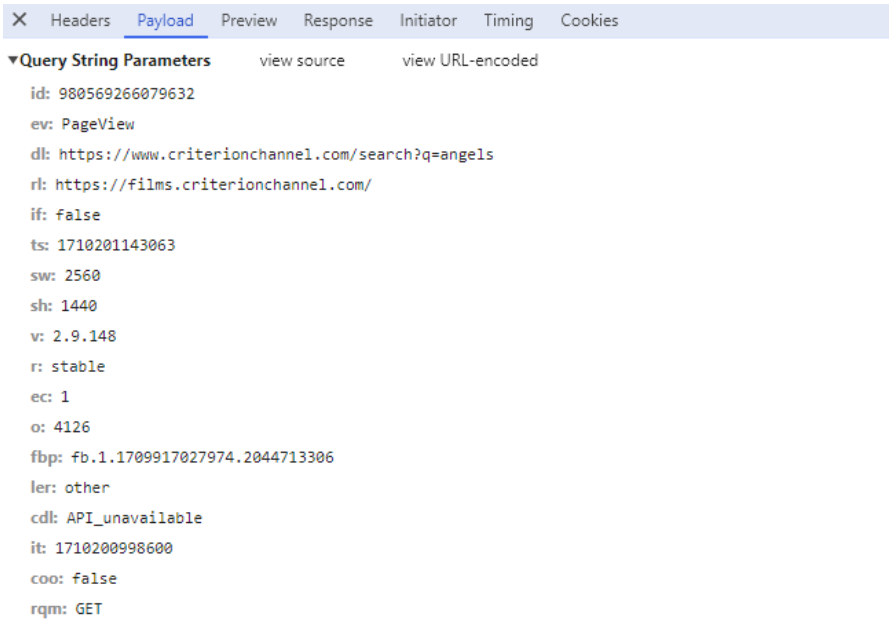

Figure 22 - Parsed URL Information from Sample Pixel Request

137. Similarly, the cookies attached to the Pixel's transmissions appear as a dense, albeit much less so, wall of text, as depicted below:

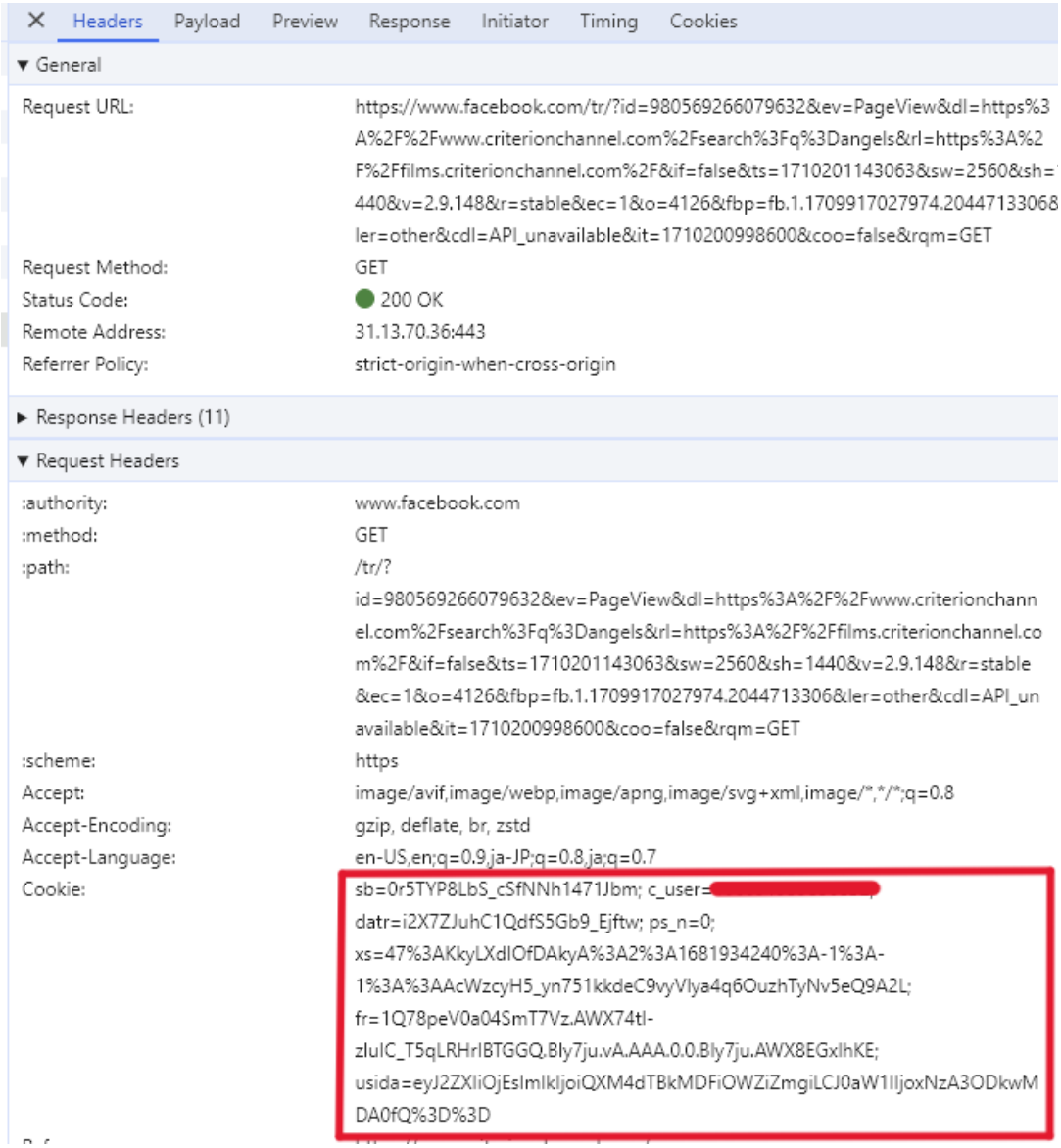

Figure 3 3- Cookie Data from Sample Pixel Request

138. However, like the URL data, the cookie data is easily parsed into more digestible format, as depicted below:

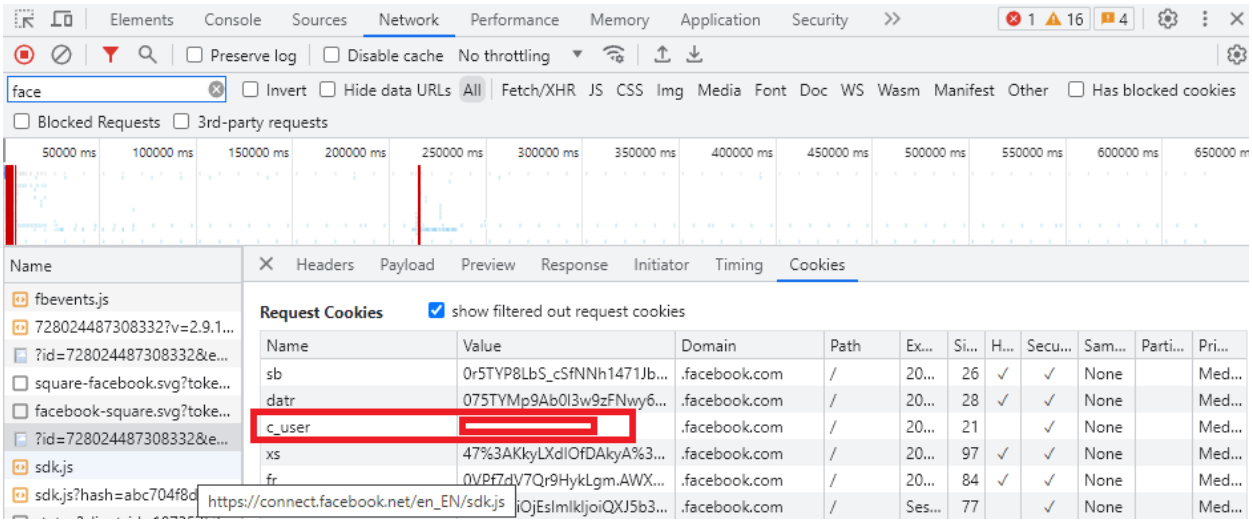

Figure 44 - Parsed Cookie Data from Sample Pixel Request

139. PII can be used by anyone who receives the Pixel transmission to easily identify a Facebook user.

140. A UID is personally identifiable information. It contains a series of numbers used to identify a specific profile, as depicted below:

Figure 5 5 - Sample UID number of test account created by Plaintiffs' counsel to investigate the Pixel, captured by a Pixel event

141. The information contained within the c_user cookie is considered PII. It contains "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."[57] Because the Facebook ID number can simply and easily

[57] *In re Nickelodeon Consumer Privacy Litigation,* 827 F.3d 262, 290 (3d Cir. 2016).

be appended to "www.facebook.com/" to navigate to the relevant user's profile, it requires no special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.[58]

142. Any person, even without in-depth technical expertise, can utilize the UID to identify owners of the UID via their Facebook profile. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual of ordinary skill and technical proficiency to easily identify a Facebook user, by simply appending the Facebook UID to www.facebook.com (e.g., www.facebook.com/[UID_here]). That step, readily available through any internet browser, will direct the browser to the profile page, and all the information contained in or associated with the profile page, for the user associated with the particular UID.eUsing the UID from *Figure 5*, appending it to the Facebook URL in a standard internet browser (here, www.facebook.com/100091959850832) will redirect the webpage straight to the Facebook profile associated with the UID, as depicted below:

[58] *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

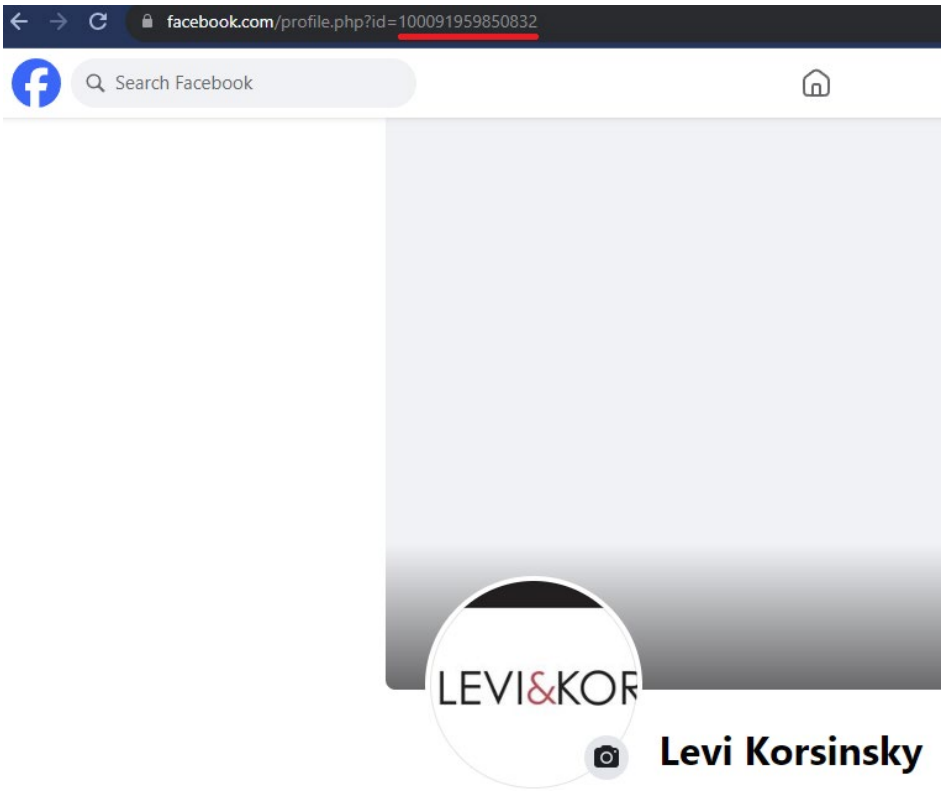

Figure 6 - Appending UID of a user to "facebook.com/" results in the user being redirected to the user's profile

143. Importantly, some Facebook profile information – name, gender, profile photo, cover photo, username, user ID (account number), age range, language, and country – are "always public."[59] No privacy setting on Facebook would allow Plaintiffs, or any user, to hide this basic information. By compelling a visitor's browser to disclose the c_user cookie alongside event data for media content, Criterion knowingly discloses information sufficiently permitting an ordinary person to identify an individual.

[59] *Control who can see what you share on Facebook*, FACEBOOK, https://www.facebook.com/help/1297502253597210 (last visited Sept. 23, 2024).

2. The Pixel as a Tracking Tool.

144. The Pixel tracks user-activity on web pages by monitoring events,[60] which when triggered, causes the Pixel to automatically send data – here, subscribers' PII – directly to Facebook.[61] Examples of events utilized by websites include: (i) a user loading a page with a Pixel installed (the "PageView event") [62] and (ii) when pre-designated buttons, like the "Watch" button, are clicked (the "SubscribedButtonClick" event).[63] The Website utilizes both.[64]

145. When a PageView and/or SubscribedButtonClick event is triggered, a "HTTP Request" is sent to Facebook (through Facebook's URL www.facebook.com/tr/).[65] This confirms that the Pixel events sent data to Facebook.

146. The HTTP Request includes a Request URL and embedded cookies such as the c_user cookie. It may also include information in its Payload,[66] such as metadata tags.

147. A Request URL, in addition to a domain name and path, contains parameters. Parameters are values added to a URL to transmit data and direct a web server to provide additional context-sensitive services, as depicted below:

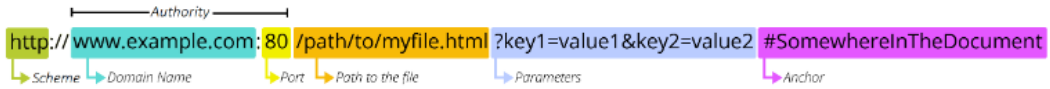

Figure 7 – Mozilla's diagram of a URL, including parameters[67]

---

[60] *Business Help Center: About Meta Pixel*, FACEBOOK https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Sept. 23, 2024).

[61] *See generally Id.*

[62] *Business Help Center: Specifications for Meta Pixel standard events*, FACEBOOK https://www.facebook.com/business/help/402791146561655?id=1205376682832142 (last visited Sept. 23, 2024).

[63] *Meta for Developers: Reference – standard events*, FACEBOOK, https://developers.facebook.com/docs/meta-pixel/reference/ (last visited Sept. 23, 2024).

[64] The presence of Pixel events can be confirmed by using the publicly available and free Meta Pixel Helper tool. *See Business Help Center: About the Meta Pixel Helper*, FACEBOOK

3. The Pixel Shares and Subscribers' PII and Video Watching Data

148. Defendant uses the Pixel as a tracking method to collect and share Website subscribers' PII with Facebook. Defendant does not disclose its data sharing practices or obtain permission from its subscribers to share their PII with Facebook.

149. Defendant shares non-anonymized, PII and web watching history containing video titles with Facebook. Defendant's disclosures include unique identifiers (the UID) that correspond to specific Facebook users. The recipient finds the PII and web watching history packaged together in a single data transmission which is easily readable by an ordinary person once the PII is packaged and delivered by the Website's tracking tools.

150. Aside from using a paid subscription business model, Defendant monetizes the Website's subscribers by disclosing subscribers' PII to Facebook in a format which allows it to make a direct connection between the identity of a subscriber and that subscriber's PII, without the consent of its subscribers and to the detriment of Plaintiffs' and Class members' legally protected privacy rights.

151. Defendant had and continues to have the choice to design the Website so that the webpage URLs did not include the titles of videos. Defendant had, and have, the choice as to whether to purposefully include more information in the Website's URLs, including to improve

---

https://www.facebook.com/business/help/198406697184603?id=1205376682832142 (last visited Sept. 23, 2024).

[65] *How We Built a Meta Pixel Inspector*, THE MARKUP https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector (last visited Sept. 23, 2024).

[66] The "request payload" (or more simply, "Payload") is data sent by a HTTP Request, normally through a POST or PUT request, where the HTTP Request has a distinct message body. Payloads typically transmit form data, image data, and programming data. *See Request Payload Verification,* SITESPECT https://doc.sitespect.com/knowledge/request-payload-trigger (last visited Sept. 23, 2024).

[67] *What is a URL?*, MOZILLA https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited on August 2, 2023).

website interaction and search engine optimization.[68] Here, Criterion chose to expose subscribers' video information so that it could benefit from the tracking and sharing of subscribers' PII.

152. Defendant also had the power to implement the Pixel in a way that shielded subscribers' sensitive information. Criterion chose, however, to transmit subscribers' unencrypted PII.[69]

153. These factual allegations are corroborated by publicly available evidence. For instance, a subscriber visits the Criterion Channel site, clicks on a pre-recorded video, such as "New Hollywood," and subsequently watches the video. After clicking on the video, the Website offers options such as watch trailer, sign up, and share.

154. Sensitive data sent to Facebook through the triggered Facebook Pixel Events are included within the parameters of the Request URL, within the Request Header, or as a Payload within the request. The specific Pixel Events implemented by Criterion sends subscribers' PII through the Request URL parameters and HTTP Headers.[70]

155. An "HTTP Header" is a field of an HTTP request or response that passes additional context and metadata about the request or response.[71] Specifically, Request Headers are a subset of HTTP Headers that are used to provide information about a request's context, so that a server can customize its response to the request or supply authentication credentials[72] to the server or

---

[68] *See Domains,* MOZ https://moz.com/learn/seo/domain (last visited Sept. 23, 2024)..

[69] *See Meta for Developers: Advanced Matching*, FACEBOOK https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching (last visited Sept. 23, 2024)..

[70] URL parameters are values that are added to a URL to cause a web server to provide additional or different services. *What is a URL?,* MOZILLA, https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL (last visited Sept. 23, 2024)..

[71] *HTTP header*, MOZILLA, https://developer.mozilla.org/en-US/docs/Glossary/HTTP_header (last visited Sept. 23, 2024)..

[72] *Id.*

otherwise provide more information about the client sending the request.[73]

156. Defendant shares with Facebook the specific streaming content requested by subscribers to the Website through Request URL parameters. This is portrayed in *Figure 8 and Figure 9* below.

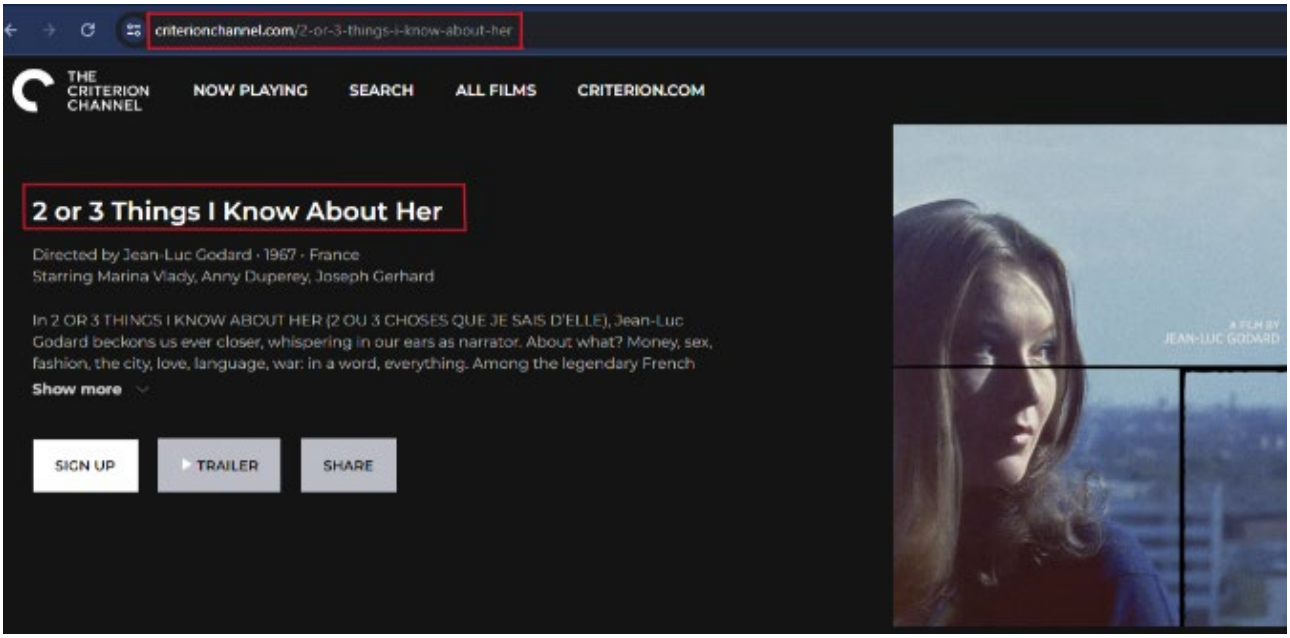

Figure 8, Sample video webpage on the Website

[73] *Id.*

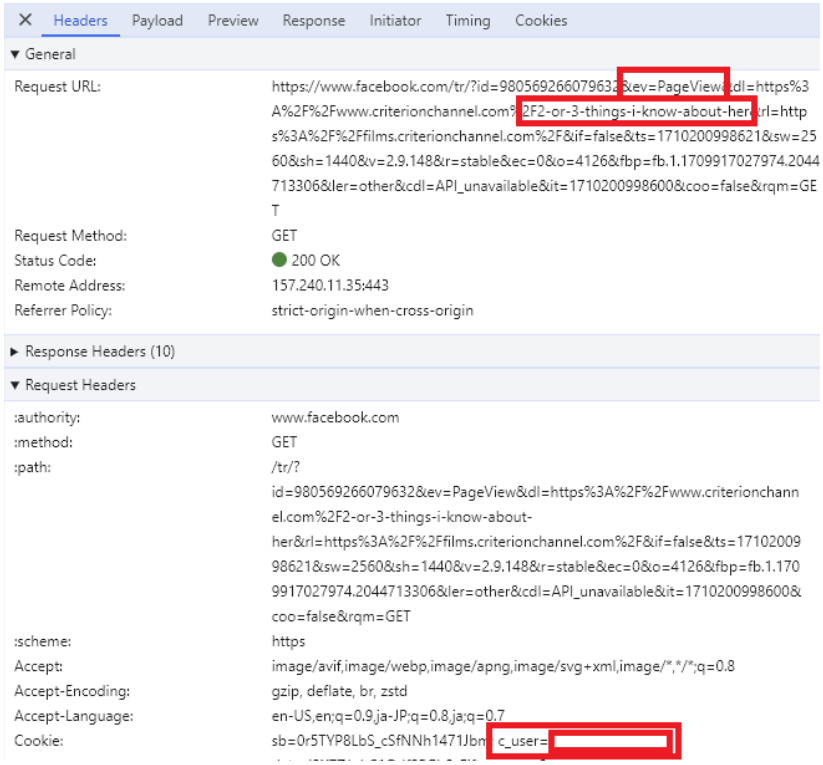

Figure 9 - Video Title included in URL parameters disclosed to Facebook through PageView Pixel Event on the Website

157. Defendant also transmits subscribers' PII to Facebook in the form of an unencrypted and unique Facebook ID number contained in the c_user cookie included in the HTTP Request Header, which can be used to find a user's personal Facebook page, as discussed in Section C(1) above.

158. The information contained within the c_user cookie is considered PII because it contains "the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."[74] Because the Facebook ID number can simply and easily be appended to "www.facebook.com/" to navigate to the relevant user's profile, it requires no

[74] *In re Nickelodeon Consumer Privacy Litigation,* 827 F.3d 262, 290 (3d Cir. 2016).

special skill or expertise to identify the user associated with the Facebook ID, and courts have regularly upheld its status as PII.[75]

4. Criterion Used the Pixel to Disclose Subscribers' Searches on the Website

159. In addition to capturing and sharing subscribers' video watching history (in violation of the VPPA) and irrespective of how the subscriber reached the web watching page, the Pixel also intercepted and shared search terms entered by Plaintiffs.

160. For example, a search for "angels" on the Website is depicted in *Figure 1* and *Figure 2* above.

161. Such search terms, while independently confidential, may also include the capturing and sharing of searches associated with subscribers' and users' video watching history, resulting in violation of the VPPA.

162. The Pixel appears on the Website, as implemented by the Defendant.

163. When a subscriber or site visitor types and submits search terms into the search bar of the Website, those search terms are intercepted and monetized by the tracking entities.

164. Plaintiffs were unaware of the Pixel's intercepting their confidential communications with the Website.

165. Plaintiffs reasonably believed that communications to the Website were made in confidence.

166. With no notice or warning as to who was intercepting and decoding the contents of their communications, Plaintiffs were not provided notice of or given an opportunity to provide consent to the Pixel's interceptions of Plaintiffs' search terms.

---

[75] *See Lebakken v. WebMD, LLC* 2022 U.S. Dist. LEXIS 201010, at *11-12 (N.D. Ga. Nov. 4, 2022); *Czarnionka v. Epoch Times Ass'n*, 2022 U.S. Dist. LEXIS 209067, at *8-10 (S.D.N.Y. Nov. 17, 2022); *Ambrose v. Boston Globe Media Partners, LLC*, 2022 U.S. Dist. LEXIS 168403, at *5-6 (D. Mass. Sept. 19, 2022).

5. Criterion Was Told The Pixel Discloses Subscribers' Data; It Knew Precisely What the Pixel Would Collect and Share

167. When a business applies with Facebook to use the Pixel, it is provided with detail about its functionality (site policy) including PII.[76]

168. To make use of the Pixel, Defendant agreed to Facebook's Business Tool Terms (the "Business Terms").

169. The Business Terms informs website owners using Facebook's tracking tools that the employment of the Pixel will result in data sharing, including with Facebook, through the automatic sharing of Pixel Event information ("Event Data") and contact information ("Contact Information").[77]

170. The Business Terms are transparent that Meta will use the Event Data and Contact Information will be processed "solely to match the Contact Information against user IDs ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[78]

171. Facebook directs parties implementing the Pixel – here, Criterion – to encrypt request information[79] *before* data can be shared.[80]

---

[76] *See Meta for Developers: Get Started*, https://developers.facebook.com/docs/meta-pixel/get-started (The Pixel "relies on Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts. Once matched, we can their actions in the Facebook Ads Manager so you can use the data . . . By default, the Pixel will track URLs visited [and] domains visited . . . .") (last visited Sept. 23, 2024)..

[77] *Meta Business Tools Terms*, FACEBOOK https://www.facebook.com/legal/terms/businesstools?paipv=0&eav=AfakosFmNyhZJOrkCsGodnMzth_uq6s403DsPEkeiKEyrj7rKyf5_t2I8wFEEUZUJlI&_rdr (last visited Sept. 23, 2024)..

[78] *Id.*

[79] This contrasts with Facebook's JavaScript Pixel, which automatically encrypts the data being sent. Criterion has specifically chosen the Pixel method which makes users' information visible. *See id.*

[80] *Id.*

172. Facebook further provides Pixel users, such as Criterion, guidance on responsible data handling, and details how data is acquired, used, and stored, including which information is shared with Facebook.

173. Facebook educates or reminds Pixel users of their responsibility to inform their subscribers of their website's data sharing, and specifically guides website owners to obtain the requisite rights, permissions, or consents, before sharing information with any third-party.[81]

174. As a sophisticated party entering into a business arrangement with another sophisticated party, Criterion was on notice of the potential privacy violations that would result from use of the Pixel, and ignored Facebook's warnings to safely handle its subscribers' data and to warn its subscribers that the Criterion Channel Website would disclose information in a manner that threatened subscribers' VPPA-protected PII.

D. The Website Lacks Informed, Written Consent Pursuant to the VPPA

175. The Website does not seek nor obtain permission from subscribers, including Plaintiffs and the Class, to share the subscribers' PII or web watching history with third parties, including Facebook.

176. The sign-up process for The Criterion Channel does not seek or obtain informed, written consent.

177. To the extent information about any of the Website's data sharing can be located, the language is not (i) presented to subscribers of the site in a transparent manner, or where it must be viewed by visitors to the website; (ii) made available as part of the sign-up process; (iii) offered to subscribers as checkbox or e-signature field, or as any form of consent; and (iv)

[81] *Business Help Center: Best Practices for Privacy and Data Use for Meta Business Tools*, FACEBOOK https://www.facebook.com/business/help/363303621411154?id=818859032317965 (last visited Sept. 23, 2024)..

presented in terms that sufficiently warn subscribers that their information, protected by the VPPA, will be shared with a third party.

TOLLING

178. The statutes of limitations applicable to Plaintiffs' and the Class's claims were tolled by Defendant's conduct and Plaintiffs' and Class members' delayed discovery of their claims.

179. As alleged above, Plaintiffs and members of the Class did not know and could not have known when they used the Website that Defendant was disclosing their information and communications to third parties. Plaintiffs and members of the Class could not have discovered Defendant's unlawful conduct with reasonable diligence.

180. Defendant secretly incorporated the Facebook Pixel into the Website, providing no indication to subscribers and visitors that their communications would be disclosed to these third parties.

181. Defendant had exclusive and superior knowledge that the tracking entities' tracking tools incorporated on its Website would disclose visitors' protected and private information and confidential communications, yet failed to disclose to visitors that by interacting with the Website, Plaintiffs' and Class members' PII would be disclosed to third parties.

182. Plaintiffs and members of the Class could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of the tracking entities' tracking tools is highly technical and there were no disclosures or other indication that would inform a reasonable consumer or Website subscriber that Defendant was disclosing and allowing the interception of such information to these third parties.

183. The earliest Plaintiffs and Class members could have known about Defendant's conduct was in connection with their investigation and the work done on their behalf in preparation of filing of this Complaint.

CLASS ACTION ALLEGATIONS

184. Plaintiffs bring this action individually and on behalf of the following Classes:

> Nationwide Class: All persons in the United States with a subscription to the Website that had their Personally Identifiable Information improperly disclosed to Facebook through the use of the Facebook Pixel (the "Class").
>
> Pennsylvania Subclass: All persons in Pennsylvania with a subscription to the Website that had their Personally Identifiable Information improperly disclosed to Facebook through the use of the Facebook Pixel (the "Pennsylvania Subclass").

185. Specifically excluded from the Class are Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

186. Plaintiffs reserve the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

187. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

188. Numerosity (Rule 23(a)(1)): At this time, Plaintiffs do not know the exact number of members of the aforementioned Class. However, given the popularity of Defendant's Website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

189. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of the Class because Plaintiffs, like all members of the Class, subscribed to, and used, the Website to watch videos, and had their PII collected and disclosed by Defendant.

190. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

191. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

192. Commonality and Predominance (Rule 23(a)(2), 23(b)(3)): There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

a. Whether Defendant collected Plaintiffs' and the Class's PII;

b. Whether Defendant unlawfully disclosed and continue to disclose the PII of subscribers of the Website in violation of the VPPA, the Federal Wiretap Act, and WESCA;

c. Whether Defendant's disclosures were committed knowingly; and

d. Whether Defendant disclosed Plaintiffs' and the Class's PII without consent.

193. Information concerning Defendant's Website's data sharing practices and subscription members is available from Defendant's or third-party records.

194. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

195. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

196. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

197. Given that Defendant's conduct is ongoing, monetary damages are insufficient and there is no complete and adequate remedy at law.

COUNT I

VIOLATION OF THE VIDEO PRIVACY PROTECTION ACT
18 U.S.C. § 2710, *et seq*.
(On Behalf of Plaintiffs and the Nationwide Class)

198. Plaintiffs hereby incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 32 and paragraphs 40 through 176.

199. Plaintiffs bring this count on behalf of themselves and all members of the Nationwide Class.

200. The VPPA provides that "a video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer shall be liable to the aggrieved person for the relief provided in subsection (d)." 18 U.S.C. § 2710(b)(1).

201. "Personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

202. A "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of pre-recorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

203. Defendant violated this statute by knowingly disclosing Plaintiffs' and other Class members' personally identifiable information to Facebook.

204. Defendant, through the Website, engages in the business of delivering video content to subscribers, including Plaintiffs and the other Nationwide Class members, and other users. The Website delivers videos to subscribers, including Plaintiffs and the other Class members, by making those materials electronically available to Plaintiffs and the other Class members on the Website.

205. Defendant is a "video tape service providers" because they curate, host, provide access to, and cause the delivery of thousands of videos on the Website, thereby "engag[ing] in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

206. Defendant solicits individuals to pay to subscribe to the Website.

207. Plaintiffs and members of the Class are "consumers" because they paid to subscribe to Defendant's Website. 18 U.S.C. § 2710(a)(1).

208. Plaintiffs and members of the Class viewed videos on the Website.

209. Defendant disclosed Plaintiffs' and Class members' personally identifiable information to Facebook. Defendant utilized the Pixel which forced Plaintiffs' web browser to transmit Plaintiffs' identifying information, like their Facebook ID, along with Plaintiffs' and Class members' event data, including the title of the videos they viewed, to Facebook.

210. Defendant knowingly disclosed Plaintiffs' and Class members' PII, which is triggered automatically through Defendant's use of the Pixel. No additional steps on the part of the Defendant, Facebook, or any third-party are required. Once the Pixel's routine exchange of information is complete, the UID that becomes available can be used by any individual to easily identify a Facebook user. *See* Section C(1) (process to identify individual using UID).

211. Plaintiffs and members of the Class did not provide Defendant with any form of consent—either written or otherwise—to disclose their PII to Facebook. Defendant failed to obtain "informed, written consent" from subscribers – including Plaintiffs and members of the Class – "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and "at the election of the consumer," either "given at the time the disclosure is sought" or "given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner." 18 U.S.C. § 2710(b)(2)(B)(i)-(ii).

212. Defendant's disclosures of Plaintiffs' and Class members' PII were not made in the "ordinary course of business" as the term is defined by the VPPA. In particular, Defendant's disclosures to Facebook were not necessary for "debt collection activities, order fulfillment, request processing, [or] transfer of ownership." 18 U.S.C. § 2710(a)(2). Instead, t Plaintiffs' and Class members' PII was used for improving marketing effectiveness.

213. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

214. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief as to Defendant; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with VPPA's requirements for protecting a consumer's PII; (iii) statutory damages of $2,500 for each violation of the VPPA pursuant to 18 U.S.C. § 2710(c); and (iv) reasonable attorneys' fees and costs and other litigation expenses.

Injunctive Relief Of Defendant's Ongoing VPPA Violations

215. An actual and immediate controversy has arisen and now exists between Plaintiffs and the putative classes they seek to represent, and Defendant, which parties have a genuine and opposing interest in and which their interests are direct and substantial. Defendant has violated, and continue to violate, Plaintiffs' and Class members' rights to protect their PII under the VPPA.

216. Plaintiffs have demonstrated that they are likely to succeed on the merits of their claims, and are thus entitled to declaratory and injunctive relief.

217. Plaintiffs have no adequate remedy at law to stop the continuing violations of the VPPA by Defendant. Unless enjoined by the Court, Defendant will continue to infringe on the

privacy rights of Plaintiffs, Class members, and the absent Class members, and will continue to cause, or allow to be caused, irreparable harm to Plaintiffs and Class members. Injunctive relief is in the public interest to protect the PII of Plaintiffs and Class members, and other consumers that would be irreparably harmed through continued disclosure of their PII.

218. Criterion completely disregards their obligation under the VPPA by loading the Pixel onto the Website and facilitating the sharing of subscribers' PII with third parties for any ordinary person to access and use.

219. Despite brazenly violating the VPPA, subscribers were provided with no notice of the employment of the Pixel and no indication of how or how much of their information was shared with third parties. Worse, in further violation of the VPPA, Defendant did not seek or obtain any form of consent from subscribers for the use of the tracking tools to share information improperly pulled from the Website.

220. This threat of injury to Plaintiffs and members of the Class from the continuous violations requires temporary, preliminary, and permanent injunctive relief to ensure their PII is protected from future disclosure.

COUNT II

VIOLATION OF THE FEDERAL WIRETAP ACT
18 U.S.C. § 2710, *et seq.*
(On Behalf of Plaintiffs and the Nationwide Class)

221. Plaintiffs hereby incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 32 and paragraphs 40 through 176.

222. Codified under 18 U.S.C. § 2510 *et seq.*, the Federal Wiretap Act prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

223. The Wiretap Act confers a civil private right of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

224. The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

225. The Wiretap Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

226. The Wiretap Act defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

227. The Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

228. Defendant is a person for the purposes of the Wiretap Act.

229. The Pixel and other tracking tools constitute a "device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

230. The confidential communications Plaintiffs had with the Website, in the form of their search terms, browsing information, and PII, were intercepted by the tracking entities and such communications were "electronic communications" under 18 U.S.C. § 2510(12).

231. Plaintiffs had a reasonable expectation of privacy in their electronic communications with the Website in the form of their search terms submitted to the Website and browsing information. Even if Plaintiffs would not have had a reasonable expectation of privacy

in the electronic communications normally, Plaintiffs' electronic communications with the Websites included descriptions and summaries of the films and/or videos they watched, searched for, requested, or subscribed to unlock access to, along with their identifying information, giving rise to a reasonable expectation of privacy pursuant to the VPPA.

232. Plaintiffs reasonably expected that third parties were not intercepting, recording, or disclosing their electronic communications with the Website.

233. Within the relevant time period, the electronic communications between Plaintiffs and the Website were intercepted by the Pixel the instant they were sent to the Website, without consent, and for the unlawful and wrongful purpose of monetizing their PII, which includes the purpose of using such private information to develop advertising and marketing strategies.

234. Interception of Plaintiffs' confidential communications with the Website occur whenever a subscriber uses the search bar within the Website, when navigating various webpages of the Website, including those containing videos.

235. At all times relevant to this complaint, Defendant's conduct was knowing, willful, and intentional, as Defendant is a sophisticated party with full knowledge regarding the functionality of the Pixel including that allowing the tracking tools to be implemented on the Website would cause the private communications of their subscribers to be shared with third parties.

236. Plaintiffs were never asked for their consent to expose their confidential electronic communications with Website to third parties. Indeed, such consent could not have been given as Defendant never sought any form of consent from Plaintiffs to intercept, record, and disclose their private communications with the Website.

237. As detailed above, the tracking entities' unauthorized interception, disclosure and use of Plaintiffs' confidential communications were only possible through Defendant's knowing, willful, or intentional placement of the tracking tools on the Website. 18 U.S. Code § 2511(1)(a).

238. Plaintiffs have been damaged due to the unauthorized interception, disclosure, and use of their confidential communications in violation of 18 U.S.C. § 2520. As such Plaintiffs are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and any profits made by the tracking entities as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; (2) appropriate equitable or declaratory relief; and (3) reasonable attorneys' fees and other costs reasonably incurred in accordance with the Terms.

COUNT III

VIOLATION OF THE PENNSYLVANIA WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTRAL ACT ("WESCA")
18 Pa. C.S.A. § 5701, *et seq.*
(On Behalf of Plaintiff McGuire and the Pennsylvania Subclass)

239. Plaintiff McGuire incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 32 and paragraphs 40 through 176.

240. Plaintiff McGuire brings this claim individually and on behalf of the members of the proposed Pennsylvania Subclass against Criterion.

241. Criterion is a "person" as defined by 18 Pa. C.S.A. § 5702.

242. WESCA prohibits any person from willfully intercepting, endeavoring to intercept, or procuring of any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication. 18 Pa. C.S.A. §§ 5701, 5703(1).

243. Criterion procured Meta's services to "intercept" Plaintiff McGuire's and Pennsylvania Subclass members' communications with Criterion, pursuant to WESCA, which

defines "intercept" as "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. C.S.A. § 5702.

244. Criterion subsequently used the contents of Plaintiff McGuire's communications with Criterion, intercepted and processed by Meta, to target users with advertising, which is prohibited under WESCA. 18 Pa. C.S.A. § 5703(2)-(3).

245. WESCA also prohibits the knowing access to obtain access to a wire or electronic communication while it is in electronic storage by intentionally accessing, or exceeding the scope of access to, a facility through which an electronic communication service is provided. 18 Pa. C.S.A. § 5741(a)(1)-(2).

246. Criterion obtained tools from Meta to intercept and/or improperly access the communications between Criterion and its Website subscribers in the conduct of its business, in violation of WESCA.

247. The devices used in this case, include, but are not limited to:

a. Criterion's own computers, which were used to add the Pixel to its webpages;

b. Criterion's servers used to host its webpages;

c. Plaintiff McGuire's and Pennsylvania Class members' personal computing devices;

d. Plaintiff McGuire's and Pennsylvania Class members' web browsers;

e. The Pixel itself;

f. Internet cookies;

g. Third-party code utilized by Criterion; and

h. Computer servers of third parties (including Meta).

248. Defendant aided in the interception of communications between Plaintiff McGuire and Pennsylvania Class members and Defendant that were subsequently redirected to and recorded by third parties without Plaintiff McGuire's or Pennsylvania Class members' consent.

249. WESCA confers a private civil cause of action to any person whose wire, electronic or oral communication is intercepted, disclosed, or used in violation thereof against "any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication." 18 Pa. C.S. § 5725(a).

250. Plaintiff McGuire and the Pennsylvania Class members are users and subscribers of Criterion's Website. Because Plaintiff McGuire and Pennsylvania Class members plan to continue to use Criterion's Website in the future, if Criterion's unfair, unlawful, and deceptive trade practices are allowed to continue, Plaintiff McGuire and Pennsylvania Class members are likely to suffer continuing harm in the future.

251. Plaintiff McGuire and members of the Pennsylvania Class members seek all relief available for violations of WESCA, including recovery of actual damages that are not less than liquidated damages computed at a rate of $100.00 a day for each day of violation or $1,000.00, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred, along with injunctive relief.

COUNT IV

INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Nationwide Class)

252. Plaintiffs incorporate by reference and re-allege each and every allegation set forth above in paragraphs 1 through 32 and paragraphs 40 through 176.

253. Plaintiffs bring this claim individually and on behalf of the members of the proposed Nationwide Class against Criterion.

254. Criterion intentionally intruded upon Class members' solitude or seclusion in that it effectively placed Meta in the middle of conversations including search terms, precise webpage locations, and PII to which it was not an authorized party.

255. Criterion's participation in Meta's tracking and interception of PII were not authorized by Plaintiffs or Class members.

256. Criterion's enabling of Meta's intentional intrusion into Plaintiffs' and Class members' internet communications including PII and their computing devices and web-browsers was highly offensive to a reasonable person in that they violated federal and state criminal and civil laws designed to protect individuals' privacy and against theft.

257. Secret monitoring of search terms, precise webpage locations, and PII is highly offensive behavior.

258. Wiretapping and the surreptitious recording of communications including PII is highly offensive behavior.

259. Public polling on internet tracking has consistently revealed that the overwhelming majority of Americans believe it is important or very important to be "in control of who can get information" about them; to not be tracked without their consent; and to be in "control[] of what information is collected about [them]." The desire to control one's information is only heightened while a person is handling PII. Plaintiffs and Class members have been damaged by Criterion's facilitation of Meta's intrusion upon their seclusion and are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful internet tracking.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the statute referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) Entry of an order for injunctive and declaratory relief as described herein, including, but not limited to requiring Defendant to immediately (i) remove the Facebook Pixel from the Website or (ii) add, and obtain, the appropriate consent from subscribers;

(e) For damages in amounts to be determined by the Court and/or jury;

(f) An award of statutory damages or penalties to the extent available;

(g) For Defendant to pay $2,500.00 to Plaintiffs and members of the Class, as provided by the VPPA, 18 U.S.C. § 2710(c)(2)(A);

(h) For pre-judgment interest on all amounts awarded;

(i) For an order of restitution and all other forms of monetary relief;

(j) An award of all reasonable attorneys' fees and costs; and

(k) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: September 27, 2024

LEVI & KORSINSKY, LLP

By: *Mark S. Reich*

Mark S. Reich (MR-4166)
Gary S. Ishimoto*
LEVI & KORSINSKY, LLP
33 Whitehall Street, Floor 17
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: mreich@zlk.com
Email: gishimoto@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming